The official voice of the Air Force Research Laboratory
news@afrl
Roundups
August 2001

AFRL awards small business contract to Ithaca firm

by Fran Crumb, Information Directorate

ROME, N.Y. — The Air Force Research Laboratory Information Directorate has awarded a $99,985 contract to Gramma Tech Inc. of Ithaca for research to enhance the security and dependability of computer systems.

The nine-month agreement, "Detecting Malicious Code in Firmware," was awarded under the federal government's Small Business Innovative Research program. "Malicious code is code that has been intentionally added to or changed in a software system with the intention of causing harm, or subverting the intended function of the system," said Michael P. Nassif, program manager in the directorate's Defensive Information Warfare Branch. "Examples include time bombs, viruses, worms and 'Trojan horses.' Malicious code in firmware is especially dangerous."

Firmware is a combination of software and hardware that includes software programs or data that has been written onto read-only memory (ROM). It includes a Basic Input/Output System (BIOS), built in software to determine what a computer can do without accessing a program from disk. BIOS is typically placed in a ROM chip that comes with the computer.

"A computer vendor may purchase a BIOS from a supplier who may insert sleeper code that extrudes critical information to a foreign government when it is triggered," said Nassif. "Even if the original BIOS can be trusted, firmware is usually implemented in writable Flash ROM, so a malicious intruder may corrupt it at any time during its life cycle. This is particularly troublesome in the arena of national defense given the amount of commercial off-the-shelf firmware needed to support the defense mission."

Gramma Tech engineers will investigate the development of a new system for semi-automatic detection of malicious code in firmware, operating on the deep structure of the code, in contrast with existing systems, which inspect only surface structure. A sophisticated querying mechanism will be used to enable detection of deep-structure patterns indicative of malicious code. A new high-level user interface will permit the analyst to easily access this querying capability to search for telltale signs of possibly malicious code, and view the relevant portion of the suspicious firmware. **@**